Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict

HANNAH LOBEL*

SUMMARY

* J.D. Candidate, The University of Texas School of Law, 2012; M.S.J., Northwestern University, 2002; B.A., Grinnell College, 1998. I owe sincere thanks to Derek Jinks for his guidance, to Dr. Herbert S. Lin for his comments on an earlier draft, and to the staff of the Texas International Law Journal for shepherding this Note to publication. My deepest gratitude to Roy Rich for his insights, encouragement, and support. All mistakes are my own.

INTRODUCTION

On June 1, 2011, Google Inc., the world's leading search engine and a major email services provider, announced on its blog that hackers in Jinan, China, had accessed the personal email accounts of "hundreds of users including, among others, senior U.S. government officials, Chinese political activists, officials in several Asian countries (predominantly South Korea), military personnel and journalists."[1] The hack was a spear-phishing campaign, meaning it targeted specific individuals with carefully crafted emails deployed to trick users into disclosing personal information like email account passwords,[2] and it had been noticed as early as February by an independent blogger who helped tip off Google.[3]

The following day Secretary of State Hillary Clinton called Google's allegation "very serious" and announced an investigation by the Federal Bureau of Investigation.[4] Chinese Foreign Ministry spokesman Hong Lei deemed Google's claim "a complete fabrication out of ulterior motives."[5] An editorial in the *Global Times*, a Chinese nationalist newspaper, elaborated, calling Google "snotty-nosed" and disgruntled about its poor market position in China.[6]

The incident was the second major hack that Google had traced back to China. In January 2010, the company announced that a "cyber attack" originating from China had tried to steal the company's intellectual property and had targeted the email accounts of Chinese human rights advocates.[7] In response, Google reversed its controversial decision to permit China to censor its search results,[8] thus dooming the company's market aspirations in the country. Google stressed that it was not the only company that had been targeted, but felt compelled to publicize the attack because of the "security and human rights implications" and the "global debate about freedom of speech."[9] A month later, the *Washington Post* reported that Google was seeking help from the National Security Agency to help bolster its defenses against future attacks.[10]

1. Eric Grosse, *Ensuring Your Information Is Safe Online*, THE OFFICIAL GOOGLE BLOG (June 1, 2011, 12:42 PM), http://googleblog.blogspot.com/2011/06/ensuring-your-information-is-safe.html.

2. Matt Richtel & Verne G. Kopytoff, *E-Mail Fraud Hides Behind Friendly Face*, N.Y. TIMES, June 2, 2011, http://www.nytimes.com/2011/06/03/technology/03hack.html.

3. Amir Efrati & Siobhan Gorman, *Google Mail Hack Blamed on China*, WALL ST. J., June 2, 2011, http://online.wsj.com/article/SB10001424052702303657404576359770243517568.html.

4. Devlin Barrett & Siobhan Gorman, *Gmail Hack Targeted White House*, WALL ST. J., June 3, 2011, http://online.wsj.com/article/SB10001424052702304563104576361863723857124.html.

5. Hong Lei, Foreign Ministry Spokesperson, Regular Press Conference at Embassy of the People's Republic of China in the United States of America (June 2, 2011), http://www.fmprc.gov.cn/eng/xwfw/s2510/t828426.htm.

6. Jonathan Watts, *China Brands Google 'Snotty-Nosed' as Cyber Feud Intensifies*, GUARDIAN, June 3, 2011, http://www.guardian.co.uk/world/2011/jun/03/china-google-cyber-warfare.

7. David Drummond, *A New Approach to China*, THE OFFICIAL GOOGLE BLOG (Jan. 12, 2010, 3:00 PM), http://googleblog.blogspot.com/2010/01/new-approach-to-china.html.

8. *Id.*

9. *Id.*

10. Ellen Nakashima, *Google to Enlist NSA to Help It Ward Off Cyberattacks*, WASH. POST, Feb. 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html.

The more recent Google incident coincided with several other high-profile cyber operations targeting U.S. corporations.[11] For example, a few months earlier hackers had infiltrated RSA Security's systems to steal data that could decode security tokens used by companies the world over to provide secure remote access to their networks.[12] The hackers then used that data to access the networks of Lockheed Martin,[13] the federal government's leading supplier of arms and information technology.[14]

These incidents coincided with a volley of announcements from the United States and China regarding cyber conflict policies. In May of 2011, the U.S. State Department released the Administration's International Strategy for Cyberspace, which indicated that the United States would consider certain cyber attacks as triggering its right to self-defense.[15] China announced the formation of an "Online Blue Army"[16] to complement its traditional Red Army.[17] Referencing China's well-known pool of homegrown hackers, one former Chinese general commented, "It is just like ping-pong. We have more people playing it, so we are very good at it."[18] The Pentagon then leaked its new, classified cyber strategy document determining that a cyber attack from a foreign nation could constitute an act of war to which the United States might respond militarily.[19] A U.S. military official characterized the policy determination more bluntly: "If you shut down our power grid, maybe we will

11. *See* Bianca Bosker, *Pentagon Considers Cyber Attacks to Be Acts of War: WSJ*, HUFFINGTON POST (May 31, 2011, 11:34 AM), http://www.huffingtonpost.com/2011/05/31/pentagon-cyber-attack-act-of-war_n_869014.html (listing recent cyber operations against Epsilon, Sony, and Lockheed Martin).

12. Christopher Drew, *Stolen Data Is Tracked to Hacking at Lockheed*, N.Y. TIMES, June 3, 2011, http://www.nytimes.com/2011/06/04/technology/04security.html. Security tokens are designed to provide security via a "two-factor authentication system[]" in which a "user account is linked to a token, and each token generates a pseudo-random number that changes periodically, typically every 30 or 60 seconds." Peter Bright, *RSA Finally Comes Clean: SecureID Is Compromised*, ARS TECHNICA, June 2, 2011, http://arstechnica.com/security/news/2011/06/rsa-finally-comes-clean-securid-is-compromised.ars. The number is generated via the combination of an algorithm and a "seed value" specific to an individual security token. *Id.* The hackers reportedly compromised seed values, which, when combined with the already-known algorithm, apparently allowed for the generation of the numbers intended to provide identity authentication. *Id.*; Stephen Pritchard, *RSA: Life After Breach*, INFOSECURITY.COM, Aug. 12, 2011, http://www.infosecurity-magazine.com/view/20076/rsa-life-after-breach-/.

13. Angela Moscaritolo, *RSA Confirms Lockheed Hack Linked to SecureID Breach*, SC MAG., June 7, 2011, http://www.scmagazineus.com/rsa-confirms-lockheed-hack-linked-to-securid-breach/article/204744.

14. Jim Wolf & Jim Finkle, *Analysis: Lockheed Hack Highlights Cyber-blame Snags*, REUTERS, May 30, 2011, http://www.reuters.com/article/2011/05/30/us-usa-defense-hackers-idUSTRE74Q6VY20110530?feedType=RSS&feedName=everything&virtualBrandChannel=11563.

15. EXEC. OFFICE OF THE PRESIDENT, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 10, 14 (May 2011) [hereinafter INTERNATIONAL STRATEGY].

16. Ye Xin, *PLA Establishes 'Online Blue Army' to Protect Network Security*, PEOPLE'S DAILY ONLINE, May 26, 2011, http://english.peopledaily.com.cn/90001/90776/90786/7392182.html.

17. L. Gordon Crovitz, *China Goes Phishing*, WALL ST. J., June 6, 2011, http://online.wsj.com/article/SB10001424052702303657404576363374283504838.html.

18. Leo Lewis, *China's Blue Army of 30 Computer Experts Could Deploy Cyber Warfare on Foreign Powers*, AUSTRALIAN, May 27, 2011, http://www.theaustralian.com.au/australian-it/chinas-blue-army-could-conduct-cyber-warfare-on-foreign-powers/story-e6frgakx-1226064132826.

19. Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J., May 31, 2011, http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

put a missile down one of your smokestacks."[20] Soon thereafter, the State Department acknowledged Administration initiatives to create "shadow" Internet and mobile-phone systems that could be used to support dissidents in countries facing communications crackdowns from oppressive regimes.[21] By June 22—just three weeks after Google reported the latest hack against it—China apparently felt compelled to clarify that the country was not at cyber war with the United States.[22] When the Pentagon officially released the unclassified version of its cyber strategy document in mid-July, it was sanitized of the bellicose posturing that accompanied the leak of the full, classified strategy document just six weeks earlier.[23]

The growing onslaught of cyber operations against U.S. companies and the escalating cyber-war rhetoric between the United States and China point up key complexities in the already fuzzy realm of "cyber war": What role does or should the private sector play in cyber conflict and what are the rules regulating private sector conduct?

Because cyber conflict is a new, largely untested, and secretive domain,[24] there is great debate about what law of war rules, if any, regulate it. States have been relatively tight-lipped about their cyber attack capabilities and reluctant to bind themselves to rules in this emerging battlefield.[25] Indeed the United States, which has of late routinely called for international cooperation in articulating regulatory norms to guide cyber policies,[26] has steadfastly refused to disclose information regarding its offensive cyber capabilities, focusing public declarations that might

20. *Id.*

21. James Glanz & John Markoff, *U.S. Underwrites Internet Detour Around Censors*, N.Y. TIMES, June 12, 2011, http://www.nytimes.com/2011/06/12/world/12internet.html?pagewanted=1&_r=1&hp.

22. Don Durfee, *China Says No Cyber Warfare with U.S.*, REUTERS, June 22, 2011, http://www.reuters.com/article/2011/06/22/us-china-usa-cyberwar-idUSTRE75L1VJ20110622.

23. *See generally* DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (July 2011) [hereinafter STRATEGY FOR OPERATING IN CYBERSPACE]; *see* Interview by Jonathan Masters with Adam Segal, Ira A. Lipman Senior Fellow for Counterterrorism and National Security Studies [hereinafter Masters Interview], COUNCIL ON FOREIGN RELATIONS, (July 21, 2011), http://www.cfr.org/cybersecurity/pentagons-cyberstrategy/p25527 (noting that the cyber strategy released by the Pentagon was "clearly an effort to downplay foreign countries' perceptions that the United States is going to militarize cyberspace"); Noah Schachtman, *Pentagon Makes Love, Not Cyber War, in New Strategy*, WIRED, July 14, 2011, http://www.wired.com/dangerroom/2011/07/make-love-not-cyber-war (commenting upon the strategy's release that "despite a drumbeat of scare talk and digital sabre-rattling in Washington, the document takes a measured, reasonable approach").

24. In 2010, U.S. Deputy Secretary of Defense William J. Lynn III announced that the Pentagon had "formally recognized cyberspace as a new domain of warfare. . . . just as critical to military operations as land, sea, air, and space." William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFF. 97, 101 (2010).

25. *See* Scott J. Shackelford, *Estonia Three Years Later: A Progress Report on Combating Cyber Attacks*, 13 J. INTERNET L. 22, 22 (2010) ("Many nations, including the United States, have found mutual benefit in the status quo strategic ambiguity.").

26. *See, e.g.*, DEP'T OF DEF., DEPARTMENT OF DEFENSE CYBERSPACE POLICY REPORT: A REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934, at 8–9 (Nov. 2011) [hereinafter CYBERSPACE POLICY REPORT] ("Significant multinational work remains to clarify the application of norms and principles of customary international law to cyberspace."); INTERNATIONAL STRATEGY, *supra* note 15, at 9 ("We will continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace . . . ."); EXEC. OFFICE OF THE PRESIDENT, CYBERSPACE POLICY REVIEW at iv (2009) [hereinafter CYBERSPACE POLICY REVIEW] ("The Nation also needs a strategy for cybersecurity designed to shape the international environment and bring like-minded nations together on a host of issues, such as . . . acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force.").

serve to shape international norms exclusively on defensive capacity.[27] The nature of the cyber domain itself fosters this secrecy by favoring stealth actions by anonymous actors.[28] Moreover, to date, it is unclear whether any cyber operation has definitively triggered the application of the law of war.[29] Thus, legal scholarship on cyber conflict is largely an exercise in crafting hypotheticals, with scholars positing varieties of cyber-scenarios and mapping current law of war principles onto them.

The Google incidents provide excellent fodder for reality-based hypothetical queries that tease out some of the complexities that arise when private companies become primary players in a legal regime geared toward states. Was a private entity critical to the nation's digital infrastructure targeted by state-sponsored hackers in order to pilfer actionable intelligence on U.S. government officials? Did an American company, increasingly shut out of the world's fastest growing Internet market, strategically escalate tensions between the United States and China by painting China as an aggressor? Did the Chinese government, driven by national security concerns, target an American company in retaliation for U.S.-backed efforts at spreading "Internet freedom"? Did an unknown third-party hack an obvious U.S. target and spoof an IP address to frame China and escalate tensions between the United States and its burgeoning superpower rival? Might Google have violated China's sovereignty in tracing the hacking activity back to Jinan province? Should Google have been allowed to strike back at the hackers targeting it? And should a major player in the United States' communications infrastructure have to rely on a blogger to notice that its systems were hacked, particularly after it already had partnered with the NSA to better defend its network after its first go-around with Chinese hackers?

This Note seeks to situate these and other inquiries regarding the private sector and cyber conflict within the law of war framework and, in doing so, identify lacunae that should be addressed in crafting a legally sound policy regarding the cybersecurity threat facing the private sector and the federal government. In Part I, I briefly characterize how scholars have mapped the law of war onto cyber conflict

27. *See* CYBERSPACE POLICY REPORT, *supra* note 26, at 5 (responding to a congressional inquiry regarding "U.S. cyber capabilities" by stating that "[t]he dynamic and sensitive nature of cyberspace operations makes it difficult to declassify specific capabilities. However, the Department has the capability to conduct offensive operations in cyberspace to defend our Nation, Allies and interests."); Masters Interview, *supra* note 23 (noting the unclassified version of the Pentagon's cyber strategy "is really entirely about defense. There is no mention on how the Pentagon might use cyberweapons in an offensive capability.").

28. *See infra* notes 43–47 and accompanying text.

29. *See* Duncan B. Hollis, *An E-SOS for Cyberspace*, 52 HARV. INT'L L.J. 374, 405 (2011) (noting lack of consensus on whether any state has violated international law by engaging in a cyber attack); Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, 41 ISR. Y.B. HUM. RTS. 113, 120–23 (2011) [hereinafter Schmitt, *Cyber Operations and the* Jus in Bello] (arguing that cyber attacks launched against Georgia during the armed conflict between Georgia and Russia in South Ossetia in August 2008 did not constitute "attacks" under international humanitarian law); Shackelford, *supra* note 25, at 26 (suggesting that the cyber attacks against Estonia in 2007, which emanated from Russia, did not rise to the level of "armed attack" to trigger the law of war); Duncan B. Hollis, *Could Deploying Stuxnet Be a War Crime?*, OPINIO JURIS (Jan. 25, 2011, 11:54 AM), http://opiniojuris.org/2011/01/25/could-deploying-stuxnet-be-a-war-crime (determining that, under some approaches to applying law of war principles to cyber attacks, the Stuxnet worm that targeted an Iranian nuclear facility, discussed *infra*, would constitute a "use of force" or "armed attack" under the U.N. Charter if it were attributable to a state).

generally, considering both *jus ad bellum* and *jus in bello* regimes.[30] This analysis is key to understanding how the ambiguities plaguing the application of the law of war to cyber conflict are further complicated when the private sector plays a role. In Part II, I consider the Obama administration's proposal to foster public-private partnerships as a means of combating cyber attacks, as well as a few current models proposed by legal scholars to address this dilemma. I then point out law of war blind spots in these political and scholarly proposals and argue that how these issues are resolved will have important implications for the development of customary international law in cyber conflicts. My primary concerns in this regard are the erosion of the state's monopoly on the use of force and the eroding standard for imputation of non-state actor conduct to states. The last section offers a brief conclusion.

I. MAPPING THE LAW OF WAR ONTO CYBER CONFLICT

In order to understand the complexities surrounding the private sector's role in cyber conflict, it is necessary to first examine how the traditional law of war maps onto cyber conflict generally. This Part first considers the threshold triggers necessary for cyber operations to implicate the law of war. It then outlines how, once the law of war is triggered, its rules apply, considering both *jus ad bellum* and *jus in bello* regimes.

A. Threshold Questions

Determining whether the law of war governs a cyber operation can be difficult to resolve with any certainty. The thresholds of applicability can be broken down into four generalized questions: (1) What is the purpose of the cyber operation? (2) Who is the perpetrator? (3) What are the consequences or intended consequences of the cyber operation? (4) Is there an ongoing armed conflict to which the cyber operation is connected? As will be seen, the answers to all of these questions may be unanswerable at the point in time when a victim seeks to calibrate and launch countermeasures.

1. What Is the Purpose of the Cyber Operation?

Offensive cyber operations can be broadly classified into two categories: computer network attacks and computer network exploitations. Computer network attacks (CNA) aim to "alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[31] Computer network exploitations (CNE), on

30. *Jus ad bellum* refers to the body of international law regulating when a state may use force against another state. *Jus in bello* refers to laws regulating the conduct of hostilities. This paper uses "law of war" as an umbrella term covering both regimes. *See* Robert D. Sloane, *The Cost of Conflation: Preserving the Dualism of* Jus ad Bellum *and* Jus in Bello *in the Contemporary Law of War*, 34 YALE INT'L. L.J. 47, 50 n.15 (2009) (explaining the usage of the terms "law of war," *jus ad bellum*, *jus in bello*, "international humanitarian law," and "law of armed conflict," and delineating between them).

31. NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 80 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [Hereinafter NRC REPORT].

the other hand, aim to extract information and "may cause no explicit disruption or destruction at all."[32] The differences are intent, effects, and the governing legal regime.

A CNE is a form of espionage and, as in the physical domain, is not barred by the law of war but rather by domestic law.[33] Thus, the law of war is not concerned with CNEs.[34] The problem in the cyber domain, however, is that a CNE is often not readily distinguishable from a CNA because its effects may not be immediately apparent and the intent may not be readily intelligible by technical means. Both CNAs and CNEs seek to take advantage of a vulnerability in a system in order to access the system and execute a payload.[35] The type of payload is what distinguishes the two operations, and that difference may be difficult to distinguish technically.[36]

Take, for example, the Stuxnet worm that crept through Windows systems for more than a year before security experts from around the globe were able to piece together clues that it was targeting Iranian uranium-enrichment centrifuges.[37] In the initial phases of deconstructing Stuxnet's code, security experts discovered that the worm was "stealing configuration and design data from [control] systems, presumably to allow a competitor to duplicate a factory's production layout."[38] Thus, Stuxnet looked like "just another case of industrial espionage."[39] But as the experts continued to chip away at what many considered the most complex malware ever discovered, they found that Stuxnet's espionage functions were actually targeting functions and that the worm also carried a destructive payload.[40] Once the worm reached its intended target—an industrial controller—it ran dual programs: one replaced the commands sent to the controller with malicious commands, while the other masked the code doing the destructive work.[41] But the experts still could not identify exactly what Stuxnet's specific purpose or specific target was. It was only after the effects of the operation became evident—after it became public that

32. David D. Clark & Susan Landau, *Untangling Attribution*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 25, 28 (National Research Council ed., 2010).

33. *See* Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 151, 156 [hereinafter Schmitt, *Cyber Operations*] (noting that it is "well accepted that the international law governing the use of force does not prohibit propaganda, psychological warfare or espionage").

34. An exception to this general rule would be a CNE gathering information prefatory to an attack during an armed conflict. In this instance, *jus in bello* rules may permit the perpetrator of a CNE to be targeted.

35. NRC REPORT, *supra* note 31, at 81.

36. *Id.*

37. The earliest version of Stuxnet was apparently released in the summer of 2009. In September 2010 an industrial-control-systems-security expert in Hamburg announced that he had reverse-engineered the virus's payload and discovered its ultimate purpose: sabotaging certain Siemens-made programmable-logic controllers operating under certain conditions. The certain controllers operating under certain conditions are now widely believed to have been those at an Iranian nuclear site. Michael Joseph Gross, *A Declaration of Cyber-War*, VANITY FAIR, April 2011, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

38. Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*, WIRED, July 11, 2011, http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1.

39. *Id.*

40. *Id.*

41. *Id.*

centrifuges had been failing in droves at the Natanz nuclear facility in Iran—that it became definitively clear that the worm had been directing the centrifuges to secretly spin out of control[42] and that Stuxnet was not only a CNE but also a CNA.

As Stuxnet shows, a state seeking to respond to a cyber operation might not know whether a cyber operation is a CNA or CNE because the state might not be able to identify the operation's purpose. The effect of this ambiguity is that the state might not know what legal regime—international or domestic—governs its behavior.

2. Who Is the Perpetrator?

In the cyber context, attribution can refer to the identification of a cyber operation's perpetrator or to the computer or location from which the operation emanates.[43] Like a cyber operation's purpose, attribution can be tricky to ascertain with certainty, particularly when it regards a perpetrator's identity.[44] The technical hurdles to attribution stem from the myriad means that cyberspace affords actors anonymity.[45] For example, tracing an internet-based cyber operation back to an IP address does not necessarily constitute identification of the perpetrator. A perpetrator might forge an IP address or use anonymizers to leave a false trail of IP addresses.[46] Even if a cyber operation is traced back to an IP address from which the operation emanates, the attacking computer might have been unwittingly co-opted by a botnet being anonymously controlled by the actual perpetrator.[47] In this instance, the computer responsible for part of the operation can be identified, but the actual actor perpetrating the operation may not be determined.

Attribution also can impact whether the cyber operation—and a response to it—is governed by a domestic law-enforcement regime or by the law of war.[48] A

42. William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

43. *See* Clark & Landau, *supra* note 32, at 25–26 ("Attribution on the Internet can mean the owner of the machine (e.g., the Enron Corporation), the physical location of the machine (e.g., Houston, Estonia, China), or the individual who is actually responsible for the actions."). My discussion of "attribution" here focuses on identifying the actual perpetrator of a cyber operation. This usage is different from a common use of "attribution" in international law to refer to the concept of attributing a non-state actor's actions to a state. Later in this Note, I refer to this latter concept as "imputation" in order to keep the two concepts distinct.

44. Rose McDermott, *Decision Making Under Uncertainty*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 227, 229 ("[U]nlike most military attacks, cyberattacks defy easy assessments of perpetrator and purpose.").

45. *See* Clark & Landau, *supra* note 32, at 26–27 (describing how the Internet's reliance on packet-switching and network-layering allows for anonymity).

46. Hollis, *supra* note 29, at 399.

47. A botnet is "a network of thousands or even millions of computers under the control of an attacker that is used to carry out a wide range of services." Tyler Moore, *Introducing the Economics of Cybersecurity: Principles and Policy Options*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 3, 6. In this regard, a botnet can serve as a "force multiplier" by allowing one actor to harness the capacity of thousands or millions of computers. *See* David Gerwitz, *10 Things You Should Know About the Pentagon's New Cyberwarfare Strategy*, ZDNET GOVERNMENT (June 2, 2011, 5:00 AM), http://www.zdnet.com/blog/government/10-things-you-should-know-about-the-pentagons-new-cyberwarfare-strategy/10429 ("[A]ny small group with a pile of PCs (or even PlayStations) can mount a hugely damaging attack, especially if they make use of zombie botnets as a force multiplier.").

48. Hollis, *supra* note 29, at 405 ("If you do not know who authored an attack, how can you know whether to treat it as a crime or an act of war?").

range of different types of actors are at work in the cyber operations realm: garden-variety criminals, non-state actors with political motivations,[49] white-hat hackers,[50] state-sponsored hackers, and military actors, to name a few. While the category that a perpetrator falls into might not definitively determine the applicable legal regime, it is an important part of the calculus. For example, a teenage resident hacking a city's electrical grid likely would be subject to domestic criminal law; a foreign state doing the same, with destructive effect, might be governed by the law of war.[51]

The attribution problem complicates not only whether the law of war applies but also how states can act in compliance with law of war rules without certainty regarding who the actual attackers are. This complication is discussed more in-depth below, but a few general examples elucidate the point. An attacker might use a "false flag" operation[52] to dupe one state into thinking it was attacked by another state, thereby instigating a catalytic conflict.[53] Or an attacker might leave a false trail that leads a victim state to retaliate against a network that, if subjected to countermeasures, could have indirect effects upon civilians, including the victim's own citizens.

3. What Are the Consequences or Intended Consequences of the Cyber Operation?

The law governing when states can resort to force, *jus ad bellum*, and the law governing states' conduct during armed conflict, *jus in bello*, were written with the kinetic realm in mind. "Use of force"[54] and "armed attack"[55]—key thresholds in *jus ad bellum*—necessarily imply physical concepts. "Armed conflict,"[56] "attack,"[57] and

49. *See* ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 31–32 (2010) (describing the "emerging trend of 'patriotic hacking'").

50. *See Definition of: white hat hacker*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,2542,t=white+hat+hacker&i=54434,00.asp (last visited Jan. 6, 2012) (defining "white-hat hackers" as the "good guys," i.e., "concerned employees or security professionals who are paid to find vulnerabilities").

51. *See* Schmitt, *Cyber Operations and the* Jus in Bello, *supra* note 29, at 131 ("[A]ny [cyber] operation by or attributable to a State which results in damage to or destruction of objects or injury to or death of individuals of another State would commence an international armed conflict.").

52. *See* Dancho Danchev, *Should a Targeted Country Strike Back at the Cyber Attackers?*, ZERO DAY, (May 10, 2010, 2:03 PM), http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194 (describing "false flag cyber operations" as "impersonating a particular country" in order to "engineer[] cyber warfare tensions by relying on the negative reputation of 'usual' suspects").

53. A catalytic conflict is one "in which a third party instigates conflict between two other parties." NRC REPORT, *supra* note 31, at 312.

54. *See* U.N. Charter art. 2, para. 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

55. *See* U.N. Charter art. 51 ("Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations . . . .").

56. Common Article 2 of the four Geneva Conventions stipulates the Conventions' application trigger as "all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties." Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 12 August 1949, art. 2, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of the Armed Forces at Sea, 12 August 1949, art. 2, 6 U.S.T. 3217, 75 U.N.T.S. 135; Geneva Convention

"acts of violence,"[58] critical concepts in *jus in bello*, do as well. Thus, some have questioned whether the law of war can or should govern cyber conflicts.[59] But this assessment has been generally rejected.[60] Though cyber operations take place in a non-physical realm, they can have physical effects such as destruction, injury, and death. A cyber network attack upon an electrical grid's network could shut a city's electricity down, causing casualties by wreaking havoc on traffic systems or cutting off life-sustaining energy to hospitals. A cyber network attack on a nuclear reactor's control system might cause a meltdown and catastrophic release of radiation. Because international law seeks to protect certain entities, namely civilians and civilian objects, from such effects, the legal regime applies in the cyber conflict realm.[61]

Thus, to translate the law of war's kinetic concepts to the cyber realm, legal scholars have generally focused on the consequences or intended consequences of a cyber network attack to determine whether *jus ad bellum* or *jus in bello* principles are implicated.[62] The specifics of when these regimes might be triggered and, if so, how they regulate conduct are discussed in-depth below. Of note here is simply that the consequences of a cyber network operation must reach a certain threshold to even implicate law of war principles.

Relative to the Treatment of Prisoners of War, 12 August 1949, art. 2, 6 U.S.T. 3316, 75 U.N.T.S. 135; and Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, art. 2, 6 U.S.T. 3516, 75 U.N.T.S. 287.

57. *See* Protocol Additional to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 51(2), Dec. 12, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I] ("The civilian population as such, as well as individual civilians, shall not be the object of attack."); *id.* art. 51(4) ("Indiscriminate attacks are prohibited."); *id.* art. 52(1) ("Civilian objects shall not be the object of attack or of reprisals."); *id.* art. 52(2) ("Attacks shall be limited strictly to military objectives."); *id.* art. 49(1) ("'Attacks' means acts of violence against the adversary, whether in offence or in defence."); *id.* art. 49(2) ("The provisions of this Protocol with respect to attacks apply to all attacks in whatever territory conducted . . . .").

58. *See id.* art. 49(1) ("'Attacks' means acts of violence against the adversary, whether in offence or in defence."); *id.* art. 51(2) ("Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.").

59. *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1031 (2010) ("Because the UN Charter was written long before the Internet existed, it was clearly not intended to encompass cyberattacks. Therefore, it is reasonable to assume that the Charter encompasses only kinetic attacks. Since cyberattacks will almost certainly not involve the use of physical force, the Charter and the contemporary [Law of Armed Conflict] probably do not apply.").

60. *See, e.g.*, Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INT'L REV. OF THE RED CROSS 365, 368–73 (2002) [hereinafter Schmitt, *Wired Warfare*] (dispelling arguments that the law of war does not apply to computer network attacks because they arose after the relevant treaty regime, are not addressed by treaty law, or apply only to kinetic conflict); CYBERSPACE POLICY REPORT, *supra* note 26, at 9 ("International legal norms, such as those found in the UN Charter and the law of armed conflict, which apply to the physical domains (i.e., sea, air, land, and space), also apply to the cyberspace domain.").

61. Schmitt, *Wired Warfare*, *supra* note 60, at 373.

62. *See generally* Schmitt, *Wired Warfare*, *supra* note 60; Schmitt, *Cyber Operations*, *supra* note 33; Paul A. Walker, *Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine*, 1 NAT'L SEC. L. BR. 33; NRC REPORT, *supra* note 31, at 67–68, 252.

4. Is There an Ongoing Armed Conflict to Which the Cyber Operation Is Connected?

Armed conflict is the threshold condition for application of *jus in bello* rules (also known as international humanitarian law (IHL) or the law of armed conflict (LOAC)).[63] While addressing "armed conflict" as a threshold of IHL application may seem repetitive given the consequences-based threshold discussed above, the two matters are actually distinct. The latter seeks to clarify that consequences must be of a certain kind to implicate both *jus ad bellum* and *jus in bello* rules. The former clarifies that cyber network attacks are regulated under *jus in bello* rules only if an armed conflict exists. The National Research Council's Committee on Offensive Information Warfare provides a helpful elaboration:

> [T]he difficult legal and ethical policy issues regarding the appropriateness of using cyberattack seem to arise mostly in a prekinetic situation, where traditional armed conflict has not yet arisen (and may never arise). In this context, decision makers must determine whether a cyberattack would be equivalent to "the use of force" or "an armed attack." . . . As for the situation in which a "kinetic" conflict has already broken out, cyberattack is just one more tactical military option to be evaluated along with other such options—that is, when U.S. military forces are engaged in traditional tactical armed conflict and except in extraordinary circumstances, there is no reason that any non-LOAC restrictions should be placed on the use of cyberattack vis-à-vis any other tactical military option.[64]

This analysis, however, is helpful only to a point. It seems to leave uncovered those cyber network attacks "in situations that fall short of actual armed conflict."[65]

Thus, the discussion of the application of *jus in bello* rules of proportionality and distinction that follows proceeds from the position that these rules apply to cyber attacks during an armed conflict in progress or when a cyber attack rises to the threshold of instigating an armed conflict and that the rules are instructive normative guides—though not legally binding—in cyber network attacks that neither occur during an armed conflict nor instigate an armed conflict. Indeed, the case for applying *jus in bello* principles in situations falling short of armed conflict is particularly compelling in the cyber realm, where the outcomes of cyber operations are more uncertain and cascading effects are more likely.[66]

B. Applying the Law of War to Cyber Conflicts Generally

The previous section examined the key thresholds that must be met to trigger the application of the law of war to cyber operations. This section provides a brief

63. *See supra* note 56.

64. NRC REPORT, *supra* note 31, at 67.

65. *Id.* at 68. The committee notes that "the relevant international law under such circumstances is poorly developed at best." *Id.* To address this gap, the committee recommends applying "the moral and ethical principles underlying the law of armed conflict to cyberattack even in situations that fall short of actual armed conflict." *Id.*

66. *See infra* notes 94–95 and accompanying text.

overview of how, once triggered, law of war principles apply to cyber network attacks. It also highlights problematic ambiguities in the cyber realm, which—as will be discussed later—are made more problematic by the private sector's involvement in cyber conflict.

1. *Jus ad Bellum*

Article 2(4) of the U.N. Charter prohibits states from "the threat or use of force against the territorial integrity or political independence of any state."[67] Scholars disagree on whether "use of force" amounts to "armed force,"[68] though there is general agreement that it does not include economic coercion.[69]

Article 2(4)'s prohibition does not indicate a remedy for states subjected to an illegal threat or use of force, rather it "merely set[s] a threshold for breach of international law."[70] Article 51, however, assures a state of its right to act in self-defense against an "armed attack."[71] The daylight between Article 2(4)'s "use of force" and Article 51's "armed attack" is another subject of debate among legal scholars.[72]

For those who see daylight, all armed attacks would amount to uses of force, but not all uses of force would trigger a state's right to self-defense. In 1999 Professor Michael Schmitt applied this dual regime to cyber network attacks, proposing six factors that could be used to determine whether a computer network attack constitutes a use of force: severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy.[73] Schmitt applied a more exacting standard, however, for computer network attacks that amount to armed attack triggering the right to self-defense under the U.N. Charter, using a consequences-based analysis to require death, injury, damage, or destruction.[74]

The confirmation hearing testimony of Lieutenant General Keith Alexander, however, indicates that the new head of the Pentagon Cyber Command conflates use of force and armed attack in the cyber realm:

67. *See supra* note 54.

68. *See, e.g.*, Schmitt, *Cyber Operations*, *supra* note 33 (noting that "armed" does not appear in Article 2(4) and citing the International Court of Justice's opinion in the *Nicaragua* case to argue that "[t]he threshold for a use of force must therefore lie somewhere along the continuum between economic and political coercion on the one hand and acts which cause physical harm on the other"); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 427–28 (using textual references to support the "the dominant view in the United States and among its major allies [which] has long been that the Article 2(4) prohibition of force and the complementary Article 51 right of self-defense apply to military attacks or armed violence").

69. *See* Schmitt, *Cyber Operations*, *supra* note 33 (noting that during the Charter's drafting "a proposal to extend the reach of Article 2(4) to economic coercion was decisively defeated").

70. *Id.* at 154.

71. *See supra* note 55.

72. Waxman, *supra* note 68, at 427 n.23.

73. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885, 914–15 (1999) [hereinafter Schmitt, *Computer Network Attack*]. These factors remain influential fence posts today. Schmitt later added a seventh factor, state responsibility. Schmitt, *Cyber Operations*, *supra* note 33, at 156.

74. Schmitt, *Cyber Operations*, *supra* note 33, at 164; Schmitt, *Computer Network Attack*, *supra* note 73, at 929.

> [I]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response.[75]

This lack of clarity is potentially compounded by the application of the doctrine of anticipatory self-defense, which is based on the idea that a state need not wait to be attacked in order to defend itself.[76] According to this doctrine, a state may act in self-defense when an attack against it is imminent, as judged by a "last feasible window of opportunity" standard.[77] Applying an anticipatory self-defense standard to the cyber realm might follow the following course:

> Consider a State's introduction of cyber vulnerabilities into another State's critical infrastructure. Such an action might amount to a use of force, but the victim-State may not react forcefully until it reasonably concludes that (1) its opponent has decided to actually exploit those vulnerabilities; (2) the strike is likely to generate consequences at the armed attack level; and (3) it must act immediately to defend itself.[78]

The clarity of such a scenario is enticing, but it is not evident that it encapsulates an analysis that can be concretely applied. For example, the standard for determining what is "imminent" is a matter of controversy, with the United States urging a more elastic notion of imminence to permit earlier self-defense actions.[79] Furthermore, evidentiary matters regarding the justification for exercising anticipatory self-defense already are problematic in the physical realm of warfare.[80] These evidentiary concerns are compounded in the cyber realm, where anonymity reigns, the opportunity for deceit is abundant, and attacks can be carried out within seconds—perhaps forcing potential victims to make quick decisions by shortchanging certainty.

2. *Jus in Bello*

As noted above, armed conflict is the trigger for application of the *jus in bello* regime.[81] When that threshold is met, or a computer network attack itself engenders

75. Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm., 11th Cong. 11 (Apr. 15, 2010), *available at* http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf, cited in Waxman, *supra* note 68, at 433.

76. Schmitt, *Cyber Operations*, *supra* note 33, at 165.

77. *Id.* at 166.

78. *Id.*

79. Waxman, *supra* note 68, at 437.

80. The weak evidence of Iraq's alleged possession of weapons of mass destruction, which was used to justify the U.S. invasion of the country in 2003, is a well-known case in point. *See generally* JOSEPH CIRINCIONE ET. AL., WMD IN IRAQ: EVIDENCE AND IMPLICATIONS (Carnegie Endowment for International Peace, 2004), *available at* http://www.carnegieendowment.org/publications/?fa=view&id=1435 (detailing weak evidence regarding Iraq's imminent threat to the United States and undue influence of policy on intelligence gathering).

81. *See supra* note 56 and text accompanying notes 63–65. Citing the International Red Cross Committee's commentaries to the Geneva Convention and the Additional Protocols, and reasoning from

a state of armed conflict,[82] one must consider whether any ensuing computer network operations are "attacks" regulated by *jus in bello*. Again a consequences-based analysis indicates that a computer network operation constitutes an "attack" when it results in "violent consequences":

> A cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilian or combatants, or damage to or destruction of objects, whether military objectives or civilian objects.
>
> A cyber operation that is intended, but fails, to generate such results would be encompassed in the concept, in much the same way that a rifle shot that misses its target is nevertheless an attack in IHL.[83]

When a computer network operation rises to this threshold of "attack," it is regulated by *jus in bello* principles. The following sections focus on two of those principles: distinction and proportionality.

a. Distinction

Parties to a conflict must distinguish between combatants and civilians. This duty, rooted in customary international law[84] and codified in Protocol I Additional to the Geneva Conventions,[85] includes the outward-looking obligation not to target civilians and civilian objects[86] and the inward-looking obligations for combatants to

---

the "underlying purposes of humanitarian law," Schmitt derives an operable definition of armed conflict as occurring: "when a group takes measures that injure, kill, damage or destroy." The term also includes actions intended to cause such results or which are the foreseeable consequences thereof. Because the issue is *jus in bello* rather than *ad bellum*, the motivation underlying the actions is irrelevant. So too is their wrongfulness or legitimacy. Thus, for example, the party that commences the armed conflict by committing such acts may be acting in legitimate anticipatory (or interceptive) self-defense; nevertheless, as long as the actions were intended to injure, kill, damage or destroy, humanitarian law governs them. Schmitt, *Wired Warfare*, *supra* note 60, at 373–74.

82. For an analysis of when cyber attacks might initiate an armed conflict, see Schmitt, *Cyber Operations and the* Jus in Bello, *supra* note 29, at 15–18. Schmitt explains that different analyses are necessary for cyber attacks that would initiate international armed conflict (either because they are launched by a state or by a non-state actor whose actions are imputable to a state) and cyber attacks that would initiate non-international armed conflict.

83. *Id.* at 6.

84. *Customary IHL: Rule 1. The Principle of Distinction Between Civilians and Combatants*, INTERNATIONAL COMMITTEE OF THE RED CROSS, http://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1 (last visited Mar. 30, 2012).

85. Additional Protocol I, *supra* note 57, art. 48 ("In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.").

86. *Id.* art. 51(2) ("The civilian population as such, as well as individual civilians, shall not be the object of attack."); *id.* art. 51(4) ("Indiscriminate attacks are prohibited."); *id.* art. 52(1) ("Civilian objects shall not be the object of attack or of reprisals."); *id.* art. 52(2) ("Attacks shall be limited strictly to military objectives.").

distinguish themselves[87] and to take precautions to protect civilians from military operations.[88]

The anonymity afforded by cyberspace makes distinction a difficult obligation with which to comply. First, the attribution problem can make it exceedingly difficult to identify a legitimate target with certainty, and cases of doubt regarding a person or object's civilian status are to be resolved in favor of civilian status.[89] As discussed earlier, a savvy cyber combatant can trick an adversary into attacking a civilian network by spoofing an IP address or having a botnet do his bidding.[90] A state must take reasonable steps to ensure its target is not a civilian or civilian object,[91] but it is unclear how this requirement will be calibrated in cyberspace.

Secondly, there are no uniforms in cyberspace. It is unclear, technically, how states could comply with this distinction obligation other than through barring use of anonymizers and other means of leaving false trails that might lead an adversary to retaliate, erroneously, against a civilian or civilian object. Lastly, at this late date in the Internet's infrastructural development, it is unlikely that a state such as the United States could take precautions against the effect of attacks on military objectives by separating military objectives from civilians and civilian objects in cyberspace. This is because of the "interconnectedness of U.S. government and civilian systems and the near-complete government reliance on civilian companies for the supply, support, and maintenance of its cyber capabilities."[92]

b. Proportionality

The principle of proportionality seeks to limit collateral damage to civilians and civilian objects when launching attacks.[93] Proportionality assessments likely will

87. *Id.* art. 44(3) ("In order to promote the protection of the civilian population from the effects of hostilities, combatants are obliged to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack.").

88. *Id.* art. 58 ("The Parties to the conflict shall, to the maximum extent feasible: (a) . . . endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives; (b) avoid locating military objectives within or near densely populated areas; (c) take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.").

89. *Id.* art. 50 ("In case of doubt whether a person is a civilian, that person shall be considered to be a civilian.") and art. 52(3) ("In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.").

90. *See supra* text accompanying notes 46–47. Also unclear is whether a state could target an innocent civilian's computer, taken over by a botnet, as directly participating in hostilities.

91. *See, e.g.*, Additional Protocol I, *supra* note 57, art. 57(2)(a)(i) ("[T]hose who plan or decide upon an attack shall . . . do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them.").

92. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1551 (2010).

93. Additional Protocol I, *supra* note 57, art. 57(2)(a)(ii)-(iii) ("[T]hose who plan or decide upon an attack shall . . . take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss or civilian life, injury to civilians and damage to civilian objects . . . [and] refrain from deciding to launch any attack which may be expected to cause

prove particularly precarious in cyberspace, where outcomes are more difficult to predict than in the physical world:

> Physical attacks at least have the "advantage" of physics and chemistry to work with. Because, say, the blast radius of a thousand-pound bomb is fairly well understood, one can predict what definitely lies outside the blast radius and what definitely lies inside. Error bands in cyberattack are much wider . . . ."[94]

Because cyberspace is such an interconnected domain, the effects of an attack "can spread unpredictably, far beyond the target and even back to the attacker."[95]

Stuxnet[96] offers an interesting look at what a proportionality assessment might look like in the cyber conflict age. *The New York Times* reported that Israel and the United States, the countries many believe to be behind the worm, tested Stuxnet first on centrifuges at Israel's Dimona complex.[97] The worm also included "'fail safe' features to limit its propagation," remained passive if an infected computer was not targeted, and was programmed to self-destruct on June 24, 2012, by "eras[ing] itself from every infected machine."[98] While such practices and features may serve operational goals of efficacy and stealth, they also indicate a concern with containing the worm's impact on non-targets. As Richard Clarke, the National Security Council's chief counter-terrorism adviser during the administrations of Presidents Clinton and Bush, told *Vanity Fair*, Stuxnet "just says lawyers all over it."[99]

II. THE LAW OF WAR IMPLICATIONS OF THE PRIVATE SECTOR'S ROLE IN CYBER CONFLICT

In Part I, I examined how the law of war maps onto cyber conflict generally and pointed out important law of war ambiguities and complexities that arise in the cyber realm. Part II examines how these ambiguities and complexities are amplified by the private sector's role in cyber conflict.

The law of war is geared toward states. The rise of asymmetric warfare, particularly the Global War on Terror, has reconfigured much law of war discourse toward analyzing the role of non-state actors such as terrorists. But there has been very little focus on the private sector's role in armed conflict. This is a dangerous blind spot in the domain of cyber conflict, both because the private sector's current

---

incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."). The principle of proportionality is regarded as customary international law. *Customary IHL: Rule 14. Proportionality in Attack*, INTERNATIONAL COMMITTEE OF THE RED CROSS, http://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule14 (last visited Mar. 30, 2012).

94. Martin Libicki, *Pulling Punches in Cyberspace*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 123, 126.

95. Patrick M. Morgan, *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 55, 61. *See also* Libicki, *supra* note 94, at 127 (noting that the "world's information systems are collectively approaching spaghetti status in terms of their interconnections and dependencies").

96. *See supra* notes 37–42 and accompanying text for a description of Stuxnet.

97. Broad, *supra* note 42.

98. Gross, *supra* note 37.

99. *Id.*

vulnerabilities implicate real national security concerns[100] and because this vulnerability could lead to the private sector or the government taking actions that impact law of war development and compliance in negative or non-strategic ways. My primary concern in this regard is the lack of legal clarity regarding the use of "active defenses" by the private sector.

Active defense is a broad and somewhat ambiguous concept.[101] One expert describes active defense as "a potpourri of techniques designed to limit the ability of others to carry out cyberattacks or help characterize and attribute past cyberattacks" and points out that the techniques "may straddle the fuzzy line between defense, espionage, and offense."[102] One form of active defenses uses trace-back technology to follow a cyber operation to its source and then actively disrupt the attack.[103] Active defenses are often described as counterstriking, countermeasures, "hacking back," or—as two cyber defense strategists put it—"Hack *us*? Hack *this* . . . ."[104] The point is that active defenses can go beyond simply warding off an attack with passive security measures like firewalls and instead involve actively attacking the attacker.[105]

The use of active defenses appears to be gaining support in the private sector as a means of combating cyber operations given the general consensus that passive defenses have failed as a deterrence strategy.[106] Advocates draw upon the law of self-defense as a legal justification for such actions, but the practice is of very uncertain legal pedigree in the domestic and international law context.[107] Nevertheless, active

100. More than half of the information technology and security executives at critical national infrastructure enterprises in fourteen countries reported experiencing large-scale distributed denial of service (DDoS) attacks and "stealthy infiltrations," with about 60 percent of them believing foreign states had been involved in the operations. STEWART BAKER ET. AL, MCAFEE/CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, IN THE CROSSFIRE: CRITICAL INFRASTRUCTURE IN THE AGE OF CYBER WAR 4 (2010). A third of respondents said monthly large-scale DDoS attacks had impacted their operations. *Id.* at 5. The 2010 Annual Threat Assessment of the Intelligence Community began by addressing the cyber threat, warning "[m]alicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication" and calling for a coordinated effort among the private sector and the federal government. DENIS C. BLAIR, DIRECTOR OF NATIONAL INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE INTELLIGENCE COMMUNITY FOR THE SENATE SELECT COMMITTEE ON INTELLIGENCE 2 (Feb. 12, 2009).

101. *See* Masters Interview, *supra* note 23 (calling what is meant by "active defense" "not really clear" and "not spelled out very clearly").

102. Libicki, *supra* note 94, at 124.

103. Jay P. Kesan & Carol M. Hayes, *Thinking Through Active Defense in Cyberspace*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 327, 328.

104. George Rattray & Jason Healey, *Categorizing and Understanding Offensive Cyber Capabilities and Their Use*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 77, 83.

105. See Clark & Landau, *supra* note 32, at 37 (describing active defenses as "a system under attack reach[ing] out and somehow disabl[ing] the attacking machine").

106. *See* Scott J. Shackelford, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, *in* CONFERENCE ON CYBER CONFLICT PROCEEDINGS 197, 200 (C. Czosseck & K. Podins eds., 2010) ("Cyberwarfare is an arms race that cannot be won by defense alone"); W. Earl Boebert, *A Survey of Challenges in Attribution*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 41, 48 (noting that the limitations of attribution and frustrations with "adverse trends in cyber security" may increase "'hack back' activity, with or without authorization"); Kesan & Hayes, *supra* note 103, at 328 (noting that passive defenses may not be effective in mitigating harm from an attack or deterring attacks).

107. *See* NRC REPORT, *supra* note 31, at 204–12 (describing the arguments for and against applying the law of self-defense in this context).

defenses are widely believed to be deployed by the private sector.[108] General Michael Hayden, former CIA director, explained the appeal of active defenses this way: "Right now, the sheriff isn't there. . . . Everybody has to defend themselves, so everyone's carrying a gun."[109]

Keeping the prospect of the private sector's use of active defenses in mind, this Part addresses the law of war implications of the private sector's role in cyber conflict. It first examines the Obama Administration's public-private partnership proposal as a means of addressing the national security concerns regarding critical national infrastructure. It also briefly outlines various proposals from legal scholars regarding the private sector's cybersecurity dilemma. It then identifies important and problematic law of war implications raised by these proposals as a means of highlighting key areas of concern regarding the development of customary law of war principles in the cyber realm.

A. The Obama Administration's Public-Private Partnership Plan

In May 2009, the Obama administration issued its Cyberspace Policy Review.[110] The report is the latest policy review in more than a decade of proposals and executive directives aimed at designing an effective policy to protect the nation's privately owned critical national infrastructure, coherently designating federal agencies' responsibilities for various private sectors, and, more recently, responding to increased cyber intrusions on businesses' networks that have resulted in billions in economic losses.[111] The report reiterated the necessity of building private-public partnerships to facilitate cyber incident information sharing and to coordinate efforts to "detect, prevent, and respond to significant cybersecurity incidents."[112]

While the report is clear about the motivations for these partnerships—national and economic security—it is ambiguous regarding how they will be structured and leaves the roles played by the government and industry undefined. For example, the report simultaneously asserts that the federal government has the "core responsibility" of defending privately owned critical national infrastructure but maintains that the private sector should retain autonomy in its approach to defending its systems. One passage indicates that the federal government will take the defensive lead, but remains sparse on details:

108. *See id.* at 207 (noting "anecdotal evidence and personal experience of committee members" that the private sector is deploying active defenses "even though such actions have never been acknowledged openly or done in ways that draw attention to them"); Kesan & Hayes, *supra* note 103, at 328 (noting that counterstriking is practiced in the IT industry); Jensen, *supra* note 92, at 1566 (noting that "there is evidence that many corporations are already using hack back as a defensive option); Danchev, *supra* note 52 (discussing the marketing of off-the-shelf software as a "commercial offensive cyber warfare solution").

109. BAKER ET. AL, *supra* note 100, at 26.

110. CYBERSPACE POLICY REVIEW, *supra* note 26.

111. For overviews of the history of the federal government's cybersecurity policy development and how responsibilities for various sectors of critical national infrastructure have been divvied among federal agencies, see Paul Rosenzweig, *The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 32, at 245, 247–50; Stephanie A. Devos, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 173, 179–90 (2010); Jensen, *supra* note 92, at 1555–61; CYBERSPACE POLICY REVIEW, *supra* note 26, at 4–5.

112. CYBERSPACE POLICY REVIEW, *supra* note 26, at v, 23.

> Most private network operators and service providers consider it to be their responsibility to maintain and defend their own networks, but key elements of the private sector have indicated a willingness to work toward a framework under which the government would pursue malicious actors and assist with information and technical support to enable private-sector operators to defend their own networks.[113]

The report noted that "changes in law and policy" might be required because "[c]urrent law permits the use of some tools to protect government but not private networks, and vice versa."[114] The report did not, however, elaborate on which laws the government had in mind and how those laws would need to change. It also noted that roles should be clearly defined, but did not go on to do so.

The report's ambiguity regarding the legal dimensions of the proposed partnerships reflects the fine line it hopes to walk in asserting government control while assuaging fears among the private sector and privacy advocates. Private companies worry about government regulation and forced "information sharing" with competitors,[115] while civil liberty advocates are concerned that this information sharing might invade individuals' privacy.[116] While the report seems at pains to address these concerns, there is little in it regarding the implications public-private partnerships could have on compliance with the law of war. Key among these concerns is the parameters of the private sector's ability to defend its networks. In the absence of effective government-managed defenses, can a private business launch countermeasures against a cyber network attack? If such active defenses are permissible, how are they to be regulated?

These lacunae carried over into the administration's 2011 legislative proposal, which aims to create a cybersecurity incident-reporting regime for the private sector.[117] The proposed legislation stipulates that the Secretary of the Department of Homeland Security may direct "countermeasures" to protect federal systems[118] from cybersecurity threats.[119] Countermeasures are defined as:

> automated actions with defensive intent to modify or block data packets associated with electronic or wire communications, Internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system

113. *Id.* at 28.

114. *Id.* at 17.

115. *See id.* at 27 (noting industry concerns about the "negative impacts from resulting shareholder concerns, market reactions, or regulatory action").

116. *See id.* at 9 (noting that "structures will be needed to help ensure that civil liberties and privacy rights are protected").

117. Department of Homeland Security Cybersecurity Authority and Information Sharing Act of 2011 (proposed legislation) [hereinafter Proposed Information Sharing Act], *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/dhs-cybersecurity-authority.pdf. In February and March of 2012, senators introduced competing cybersecurity bills. For analysis of the legislative proposals' private-sector information-sharing provisions, see generally Paul Rosenzweig's posts on Lawfare, available at www.lawfareblog.com/author/paul.

118. "Federal systems" are defined as "all information systems owned, operated, leased, or otherwise controlled by an agency, except for national security systems or those information systems under the control of the Department of Defense." *Id.* § 242(9).

119. *Id.* § 244(a)(1).

> from cybersecurity threats, conducted on an information system or information systems owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected.[120]

The proposed legislation does not indicate that the federal government may engage in these countermeasures to protect private entities other than those providing services to federal systems, nor does it indicate whether private entities can take these measures themselves.[121] Instead, it directs the Secretary to "develop a national cybersecurity incident response plan . . . in collaboration . . . with owners and operators of critical national infrastructure . . . based on applicable law, that describe the specific roles and responsibilities of governmental and private entities during cyber incidents."[122]

Other recent policy documents released by the Administration have not shed light on these ambiguities. For example, the State Department's May 2011 International Strategy for Cyberspace reiterates the need to partner with the private sector, but does not provide clarity regarding how private-public partnerships could be implemented in compliance with the law of war.[123] The Pentagon's recent Strategy for Operating in Cyberspace lists partnering with the private sector as one of its five key "strategic initiatives"; it also notes the Department of Defense's use of "active cyber defense . . . to discover, detect, analyze, and mitigate threats and vulnerabilities."[124] But it does not address how these public-private partnerships could be constituted in a manner that adequately considers law of war issues nor does it address the likely use of active defenses by the private sector. One document, the Cyberspace Policy Report the Pentagon prepared for Congress in November 2011, provides perhaps the most considered treatment of law of war issues in the cyber realm that has been released of late, but it does not address how these issues

120. *Id.* § 242(4).

121. I identified only one source indicating that the federal government might regard the private sector as having such power, so far as critical national infrastructure is concerned. The Department of Homeland Security's 2009 National Infrastructure Protection Plan outlines the public-private partnership between the federal government and "critical infrastructure and key resources," focusing on coordinating responses to a terrorist attack or other catastrophe. The report defines the "protection" envisioned by the plan to include "a wide range of activities, such as improving security protocols, hardening facilities, building resiliency and redundancy, incorporating hazard resistance into facility design, initiating *active* or passive *countermeasures*, installing security systems, leveraging 'self-healing' technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, business continuity planning, and restoration and recovery actions, among various others." DEPT. OF HOMELAND SEC., THE NATIONAL INFRASTRUCTURE PROTECTION PLAN 1 (2009) (emphasis added). Though the report does not specify who is providing this protection, many of the included activities are those that likely would be implemented by the private entity itself.

122. Proposed Information Sharing Act, *supra* note 117, § 243(c)(9).

123. INTERNATIONAL STRATEGY, *supra* note 15, at 13. The report does include other important statements on the law of war. As mentioned earlier, it provides a clear policy statement that a cyber network attack could trigger the right to self-defense. *See supra* note 15 and accompanying text. It also makes clear that the administration does not regard it as necessary to "reinvent" customary international law to address cyber conflict issues but rather intends to work within the current framework to build consensus regarding how those norms apply in the cyber conflict realm, thus indicating that it does not deem a separate treaty necessary to address the issue. *Id.* at 9.

124. STRATEGY FOR OPERATING IN CYBERSPACE, *supra* note 23, at 8–9.

are implicated by the private sector's role in cyber conflict or the Administration's proposal to foster public-private partnerships.[125]

B. Scholarly Proposals to Protect the Private Sector

Not surprisingly, international law scholars have focused more explicitly on law of war issues regarding the private sector in cyber conflict. This section briefly introduces a few ideas circulating in the current scholarship before discussing, generally, some of the problematic implications of both policy and scholarly treatments of the private sector's role in cyber conflict.

One proposal is for government to regulate the private sector's use of active defenses.[126] This idea envisions some type of tort liability that would protect innocent third parties who fall victim to the private sector's misfires.[127] Government regulation would aim to ensure necessary and proportionate countermeasures and require a certain accuracy rating regarding attribution confidence to permit the use of countermeasures.[128] Related to this proposal is the idea that a government-based entity could be created to pursue countermeasures on behalf of the private sector.[129]

Other proposals reach back to earlier legal mechanisms granting private actors the right to use similar defenses. For instance, one proposal suggests issuing "letters of licensing" akin to letters of marquee and reprisal that grant private actors the right to pursue "threat neutralization" under certain circumstances.[130] Another envisions a system built upon the law of the sea's Duty to Assist, whereby a cyber network attack victim could send out an "e-SOS" and certain authorized private entities such as internet service providers could respond.[131] One proposal goes rather far, pushing the idea of a "Cyberwar National Guard" that would require cyber-savvy individuals in the private sector to help bolster defenses of critical national infrastructure.[132] Another takes a tamer approach, arguing that the government should set regulatory security standards for private entities and that the executive should have the authority to defend vulnerable private entities with active defenses.[133]

C. The Law of War and the Private Sector's Role in Cyber Conflict

The political and scholarly proposals detailed above respond to real concerns about the national security threat posed by vulnerabilities in the cyber defenses of privately owned critical national infrastructure. But they also reveal blind spots that should be addressed as norms regarding cyber conflicts begin to materialize.[134]

125. *See generally* CYBERSPACE POLICY REPORT, *supra* note 26.

126. Kesan & Hayes, *supra* note 103, at 328.

127. *Id.* at 329.

128. *Id.* at 331.

129. NRC Report, *supra* note 31, at 7.

130. *Id.* at 208.

131. Hollis, *supra* note 29, at 378–79.

132. Brenner & Clarke, *supra* note 59, at 1063–67.

133. Jensen, *supra* note 92, at 1563–68.

134. *See* Rosenzweig, *supra* note 111, at 245 (warning of the dangers of making "critical decisions that may set precedent . . . in an ad hoc manner . . . without the benefit of either the time or inclination for a

Careful attention to these issues is particularly important given the unlikelihood that states will come together to craft a new treaty delineating cyber conflict rules.[135] Rather, it seems much more likely that this area of the law of war will develop via customary international law,[136] with the applicable rules established by state practice and the articulation by states of norms they regard as legally binding.[137]

The final sections of this Note identify and discuss two key blind spots: an erosion in the state's monopoly on the use of force and an erosion in the standard of imputation.

1. Erosion of the State's Monopoly on the Use of Force

The state's monopoly on the use of force serves a key function in law of war compliance. By maintaining control of who can use violence on behalf of the state, the state is able to institutionalize *jus in bello* rules via clear rules of engagement for its military forces and the use of trained military lawyers specialized in the field. The military's internal justice system also uniquely reinforces the institutionalization of the *jus in bello* regime by punishing breaches in those rules.[138]

The problem in the context of the private sector and cyber conflict is two-fold. First, the rules themselves are unclear. Second, the private sector lacks the kind of organizational structure and institutional competence that facilitates compliance with law of war rules.[139] Cyber conflict is a new war domain, with unique obstacles to applying existing norms. As discussed above, proportionality assessments are made difficult by the uncertain outcomes and cascading effects of cyber operations. Technical attribution problems make distinction a more onerous and perhaps impossible affair. Added to this fuzziness in the rules is the fact that military commanders and lawyers do not yet have an experiential basis to draw from in applying the rules.[140]

broader and comprehensive consideration of the policy implications of the decisions").

135. *See* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW 5 (Peter Berkowitz ed., 2011), *available at* http://www.hoover.org/taskforces/national-security/challenges (explaining that powerful states' interests are not sufficiently aligned to motivate them to hash out a treaty); Schmitt, *Cyber Operations*, *supra* note 33, at 177 (noting that "it is highly unlikely that any meaningful treaty will be negotiated to govern cyber operations in the foreseeable future"); *see also supra* note 123.

136. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW: SOURCES OF INTERNATIONAL LAW § 102(2) (1987) (defining customary international law as "result[ing] from a general and consistent practice of states followed by them from a sense of legal obligation").

137. *See* Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, Keynote Address at the 2011 Harvard National Security Journal Symposium: Cybersecurity: Law, Privacy, and Warfare in a Digital World (Mar. 4, 2011), *available at* http://harvardnsj.com/2011/04/the-developing-legal-framework-for-defensive-and-offensive-cyber-operations (noting that how the U.S. armed forces conduct cyber operations "will significantly influence the development of customary international law"); INTERNATIONAL STRATEGY, *supra* note 15, at 9 (articulating the Obama Administration's intention to focus on the "development of norms for state conduct in cyberspace").

138. *See* LAURA A. DICKINSON, OUTSOURCING WAR & PEACE 171 (2011) (describing judge advocates' roles in "protecting the public values that are embedded in military rules").

139. *See generally id.* at 144–95 (applying organizational theory to illustrate the obstacles to IHL compliance by private contractors in Iraq).

140. NRC REPORT, *supra* note 31, at 271–72 ("[W]hen there is little or no experience on which to draw, the congruence between the course of action proposed by commanders and what the lawyers would say is more likely to break down.").

The already difficult problem of institutionalizing operable rules in the cyber domain is further complicated if the private sector is deputized to use active defenses. Private entities face the same fuzzy rules, but have no background in the law of war or experience in armed conflict upon which to draw. More importantly, a private entity's primary motivation is likely not national security but rather the corporate bottom line. A state military can enforce the unity of command principle of war, which ensures that a single commander is directing forces in service of a common purpose,[141] that is, the nation's security. If the private sector uses active defenses against a foreign state or individuals acting on a foreign state's behalf, it may not be clear whether private or public interests are at stake.[142] Given the fact that the vast majority of cyber operations are essentially corporate espionage or criminal ventures,[143] this is a real concern. The private sector might not only erode the state's monopoly on the use of force, but also use that force in service of ends that do not serve the public interest.

2. Erosion of the Standard of Imputation

The post-September 11, 2001, international law regime already has seen the lowering of the standard for imputing to a state liability for private conduct.[144] Once a test of whether a state exercised effective or overall control over the non-state actor, the emerging standard now appears to be whether a state "harbored" or "supported" the non-state actor.[145] Given the difficulty of technical attribution in the cyber domain, some scholars are pushing the idea that imputation standards should follow this trend in relaxation in order to lift the "veil of plausible deniability" that allows states to "escape accountability" by hiding behind private hackers.[146]

The call for a relaxed standard is likely motivated by the belief that Russia and China are tapping their native hacking talent to launch a relentless stream of cyber attacks against the United States.[147] But in the rush to impute liability, this analysis misses two crucial points. The first is that the United States is no innocent. Rather, the United States is viewed as the "number one source of cyber threats" in the

141. Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 CHI. J. INT'L L. 511, 516 (2004–05) (citing Joint Chiefs of Staff's *Joint Publication 3-0 Doctrine for Joint Operations*).

142. Indeed, as discussed earlier, it also may not be clear whether public or private interests are being targeted.

143. *Talk of the Nation, Cyber Attacks May Be "Acts of War"*, NAT'L PUB. RADIO (June 3, 2011), *available at* http://www.npr.org/2011/06/03/136925541/cyber-attacks-may-be-acts-of-war.

144. Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHI. J. INT'L L. 83, 83–84.

145. *Id.* at 88–90.

146. *See, e.g.*, Shackelford, *supra* note 106, at 198; Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 7 (2009) (arguing that attribution problems "perpetuate the response crisis" in which states find themselves).

147. *See* Waxman, *supra* note 68, at 456 (noting reports that Russia and China "exploit informal relationships with private actors (i.e., 'citizen hackers') to conduct attacks and collect intelligence in cyberspace"). For an analysis calling into question the Chinese army's alleged widespread use of the country's hacker community, see NORTHMAN GRUMMAN, CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION 7 (Oct. 9, 2009).

world.[148] More importantly to developing sound law of war rules, however, is that a relaxed standard of imputation would likely confound the main underlying purpose of attribution, which is to properly identify the perpetrator and make sure that counterstrikes are directed at the right actors. Until the technical side of attribution develops to a point that instills confidence,[149] the best course is to maintain a stricter standard for imputation. This better serves the goals of international law of protecting civilians from harm and suffering. It also will serve as a disincentive to those non-state actors seeking to exploit a relaxed imputation standard by pursuing "false flag" operations or other techniques that turn innocents into virtual human shields.

CONCLUSION

The foregoing analysis does not seek to hinder policy-makers from crafting effective policies to protect the private sector from cyber attacks capable of wreaking catastrophic devastation. It is, however, meant to point out critical lacunae in the current thinking on the subject. The norms to which states profess to be obligated and the practices they pursue will be critical to establishing the rules in this emerging war domain. A coherent and sound policy must be tailored to address both national security interests and the underlying protective goals of international law.

148. Hollis, *supra* note 29, at 401.

149. *See* CYBERSPACE POLICY REPORT, *supra* note 26, at 4 (emphasizing the Pentagon's focus on improving its "attribution capabilities").